

A functional view of upper bounds on codes

Alexander Barg^{1,2} and Dmitry Nogin²

¹ *Department of ECE/ISR
University of Maryland
College Park MD 20742, USA*

² *Dobrushin Math. Laboratory
Institute for Information Transmission Problems
Bol'shoj Karetnyj 19, Moscow 101447, Russia*

E-mails: {abarg@umd.edu, nogin@iitp.ru}

Functional and linear-algebraic approaches to the Delsarte problem of upper bounds on codes are discussed. We show that Christoffel-Darboux kernels and Levenshtein polynomials related to them arise as stationary points of the moment functionals of some distributions. We also show that they can be derived as eigenfunctions of the Jacobi operator.

Keywords: Delsarte problem, Jacobi matrix, moment functional, stationary points

1. Introduction

In the problem of bounding the size of codes in compact homogeneous spaces, Delsarte's polynomial method gives rise to the most powerful universal bounds on codes. Many overviews of the method exist in the literature; see for instance Levenshtein [1]. In this note, which extends our previous work [2] we develop a functional perspective of this method and give some examples. We also discuss another version of the functional approach, a linear algebraic method for the construction of polynomials for Delsarte's problem. Our main results are new constructions of Levenshtein's polynomials.

Let \mathfrak{X} be a compact metric space with distance function τ whose isometry group G acts transitively on it. The zonal polynomials associated with this action give rise to a family of orthogonal polynomials $\mathcal{P}(\mathfrak{X}) = \{P_\kappa\}$ where $\kappa = 0, 1, \dots$ is the total degree. These polynomials are univariate if G acts on \mathfrak{X} doubly transitively (the well-known examples include the

Hamming and Johnson graphs, their q -analogs and other Q -polynomial distance-regular graphs; the sphere $S^{d-1} \in \mathbb{R}^d$) and are multivariate otherwise.

First consider the univariate case. Then for any given value of the degree $\kappa = i$ the family $\mathcal{P}(\mathfrak{X})$ contains only one polynomial of degree i , denoted below by P_i . Suppose that the distance on \mathfrak{X} is measured in such a way that $\tau(x, x) = 1$ and the diameter of \mathfrak{X} equals -1 (to accomplish this, a change of variable is made in the natural distance function on \mathfrak{X}). We refer to the model case of $\mathfrak{X} = S^{d-1}$ although the arguments below apply to all spaces \mathfrak{X} with the above properties. Let $\langle f, g \rangle = \int_{-1}^1 fg d\mu$ be the inner product in $L_2([-1, 1], d\mu)$ where $d\mu(x)$ is a distribution on $[-1, 1]$ induced by a G -invariant measure on \mathfrak{X} . Let $\mathcal{F}(\cdot) \triangleq \langle \cdot, 1 \rangle$ be the moment functional with respect to $d\mu$. We assume that this distribution is normalized, i.e., that $\mathcal{F}(1) = 1$.

Let C be a code, i.e., a finite collection of points in \mathfrak{X} . By Delsarte's theorem, the size of the code C whose distances take values in $[-1, s]$ is bounded above by

$$|C| \leq \inf_{f \in \Phi} f(1)/\hat{f}_0, \quad (1)$$

where

$$\Phi = \Phi(s) \triangleq \{f : f(x) \leq 0, x \in [-1, s]; \quad \hat{f}_0 > 0, \quad \hat{f}_i \geq 0, i = 1, 2, \dots\} \quad (2)$$

is the cone of positive semidefinite functions that are nonpositive on $[-1, s]$ (here $\hat{f}_i = \langle f, P_i \rangle / \langle P_i, P_i \rangle$ are the Fourier coefficients of f).

2. Functional approach

The choice of polynomials for problem (1)-(2) was studied extensively in the works of Levenshtein [4–6]. In this section we give a new construction of his polynomials and their simplified versions.

2.1. Notation.

Let V be the space of real square-integrable functions on $[-1, 1]$ and let V_k be the space of polynomials of degree k or less. Let $p_i = P_i / \langle P_i, P_i \rangle$, $i = 0, 1, \dots$ be the normalized polynomials. The polynomials $\{p_i\}$ satisfy a three-term recurrence of the form

$$\begin{aligned} xp_i &= a_i p_{i+1} + b_i p_i + a_{i-1} p_{i-1}, \\ i &= 1, 2, \dots; p_{-1} = 0, p_0 = 1; a_{-1} = 0. \end{aligned} \quad (3)$$

In other words, the matrix of the operator $x : V \rightarrow V$ (multiplication by the argument) in the orthonormal basis is a semi-infinite symmetric tridiagonal matrix, called the Jacobi matrix. Let $X_k = E_k \circ x$ where $E_k = \text{proj}_{V \rightarrow V_k}$, and let J_k be the $(k+1) \times (k+1)$ submatrix of J ,

$$J_k = \begin{bmatrix} b_0 & a_0 & 0 & 0 & \dots & 0 \\ a_0 & b_1 & a_1 & 0 & \dots & 0 \\ 0 & a_1 & b_2 & a_2 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & a_{k-1} \\ 0 & 0 & \dots & \dots & a_{k-1} & b_k \end{bmatrix}.$$

Example 2.1. (a) For instance, let \mathfrak{X} be the binary n -dimensional Hamming space. Then $p_i(x) = \tilde{k}_i(n/2(1-x))$, where $\tilde{k}_i(z)$ is the normalized Krawtchouk polynomial. The polynomials $p_i(x)$ are orthogonal on the finite set of points $\{x_j = 1 - (2j/n), j = 0, 1, \dots, n\}$ with weight $w(x_j) = \binom{n}{j} 2^{-n}$ and have unit norm. In this case,

$$a_i = (1/n)\sqrt{(n-i)(i+1)}, \quad b_i = 0, \quad 0 \leq i \leq n. \quad (4)$$

(b) Let \mathfrak{X} be the unit sphere in d dimensions. Then $p_i(x)$ are the normalized Gegenbauer polynomials; in this case

$$a_i = \sqrt{\frac{(n-i+2)(i+1)}{(n+2i)(n+2i-2)}}, \quad b_i = 0, \quad i = 0, 1, \dots$$

It is well known [7, p.243] that for $k \geq 1$ the spectrum of X_k coincides with the set $\mathcal{X}_{k+1} = \{x_{k+1,1}, \dots, x_{k+1,k+1}\}$ of zeros of p_{k+1} . Below we denote the largest of these zeros by x_{k+1} . Let

$$K_k(x, s) \triangleq \sum_{i=0}^k p_i(s) p_i(x) \quad (5)$$

be the k -th reproducing kernel. By the Christoffel-Darboux formula,

$$(x-s)K_k(x, s) = a_k(p_{k+1}(x)p_k(s) - p_{k+1}(s)p_k(x)). \quad (6)$$

In particular, if $s \in \mathcal{X}_{k+1}$ then $X_k K_k(x, s) = s K_k(x, s)$. Note that $K_k(x, y)$ acts on V_k as a delta-function at y :

$$\langle K_k(\cdot, y), f(\cdot) \rangle = f(y). \quad (7)$$

2.2. Construction of polynomials.

Without loss of generality let us assume that $f(1) = 1$. Then (1) is equivalent to the problem

$$\sup\{\mathcal{F}(f), f \in \Phi\}.$$

Let us restrict the class of functions to V_n . By the Markov-Lucas theorem [8, Thm. 6.4], a polynomial $f(x)$ that is nonpositive on $[-1, s]$ can be written in the form

$$f_n(x) = (x-s)g^2 - (x+1)\phi_1^2 \quad \text{or} \quad f_n(x) = (x+1)(x-s)g^2 - \phi_2^2$$

according as its degree $n = 2k+1$ or $2k+2$ is odd or even. Here $g, \phi_1 \in V_k, \phi_2 \in V_{k+1}$ are some polynomials. Below the negative terms will be discarded. We use a generic notation c for multiplicative constants chosen to fulfill the condition $f(1) = 1$.

2.2.1. The MRRW polynomial.

Restricting our attention to odd degrees $n = 2k+1$, let us seek $f(x)$ in the form $(x-s)g^2$. Let us write the Taylor expansion of \mathcal{F} in the “neighborhood” of g . Let $h \in V_k$ be a function that satisfies $\|h\| \leq \varepsilon$ for a small positive ε and the condition $h(1) = 0$. We obtain

$$\begin{aligned} \mathcal{F}((x-s)(g+h)^2) &= \mathcal{F}((x-s)g^2) + \langle (x-s)(g+h), g+h \rangle - \langle (x-s)g, g \rangle \\ &= \mathcal{F}(f) + \mathcal{F}'(h) + 1/2 \langle \mathcal{F}''h, h \rangle, \end{aligned}$$

where $\mathcal{F}' = 2(x-s)g, \mathcal{F}'' = 2(x-s)$ are the Fréchet derivatives of \mathcal{F} . This relation shows that for f to be a stationary point of \mathcal{F} , the function g should satisfy $d\mathcal{F} = 2\langle g, (x-s)h \rangle = 0$ for any function h with the above properties. First assume that $s = x_{k+1}$. Then by (6), a stationary point of \mathcal{F} is given by $g = K_k(x, s)$, and we obtain f in the form

$$f_n(x) = c(x-s)(K_k(x, s))^2.$$

Since $\hat{f}_0 = 0$, conditions (2) are not satisfied; however, it is easy to check that they are satisfied if $x_k < s < x_{k+1}$. For all such s , the polynomial f_n is a valid choice for problem (1), yielding

$$|C| \leq -\frac{1-s}{a_k p_{k+1}(s) p_k(s)} K_k^2(1, s). \quad (8)$$

The polynomial f_n was used by McEliece *et al.* [9] and Kabatiansky and Levenshtein [10] to derive their well known upper bounds on codes.

2.2.2. Levenshtein polynomials, $n = 2k + 1$.

So far in our optimization we did not use the condition $h(1) = 0$. To use it, let us write $h = (1 - x)h_1$, $h_1 \in V_{k-1}$ and repeat the above calculation. We find that stationary points of \mathcal{F} should satisfy

$$d\mathcal{F}^{(-)} = 2\langle (x - s)g, (1 - x)h_1 \rangle = 0,$$

where $\mathcal{F}^{(-)}(\cdot) = \int \cdot (1 - x)d\mu$ is the moment functional with respect to the distribution $d\mu^{(-)}(x) = (1 - x)d\mu(x)$. A stationary point of $\mathcal{F}^{(-)}$ is given by the reproducing kernel $K_k^-(x, s)$ with respect to this distribution:

$$K_k^-(x, s) = \sum_{i=0}^k p_i^-(s)p_i^-(x), \quad (9)$$

where $\{p_i^-(x), i = 0, 1, \dots\}$ is the corresponding orthonormal system. To find the polynomials $p_i^-(x)$ observe that

$$\mathcal{F}^{(-)}(p_i^- p_j^-) = \mathcal{F}(p_i^-(x)p_j^-(x)(1 - x)) = \delta_{i,j}$$

is satisfied for $p_i^-(x) = K_i(1, x)/(a_i p_{i+1}(1)p_i(1))^{1/2}$. Indeed, if $j < i$ then the function $(1 - x)K_i(1, x)$ is in the subspace spanned by p_{i+1}, p_i and thus is orthogonal to $K_j(1, x)$. To conclude, the function sought can be taken in the form

$$f_n^-(x) = c(x - s)(K_k^-(x, s))^2.$$

2.2.3. Levenshtein polynomials, $n = 2k + 2$.

In this case we seek the polynomial in the form $f_n = (x - s)(x + 1)g^2$. The necessary condition for the stationary point takes the form $\mathcal{F}^\pm((x - s)gh) \triangleq \langle (x - s)(1 - x^2)g, h \rangle = 0$. From this, $g = K_k^\pm(x, s)$ where the kernel K_k^\pm is taken with respect to the distribution $d\mu^{(\pm)}(x) = (1 + x)(1 - x)d\mu(x)$. The corresponding orthogonal polynomials $p_i^\pm(x)$ are also easily found: up to normalization they are equal

$$p_i^\pm(x) = K_i(x, -1)p_{i+1}(1) - K_i(x, 1)p_{i+1}(-1).$$

Then

$$f_n^\pm(x) = c(x - s)(x + 1)(K_k^\pm(x, s))^2.$$

Let x_k^\pm be the largest root of $p_k^\pm(x)$ (resp. of $p_k^\pm(x)$). Then $f_{2k+1}^-(x) \in \Phi$ if $x_k^+ \leq s \leq x_{k+1}^-$ and $f_{2k+2}^\pm(x) \in \Phi$ if $x_{k+1}^- < s < x_{k+1}^+$.

Remarks.

1. The polynomials f_n^-, f_n^\pm were constructed and applied to coding theory by Levenshtein [4–6]. Polynomials closely related to them were studied

in a more general context in the works of M. G. Krein *et al.*; see Krein and Nudelman [8]. The orthogonal systems $\{p_i^-\}, \{p_i^\pm\}$ are sometimes called *adjacent polynomials* of the original system $\{p_i\}$.

2. The stationary points found above are not true extremums because the second differential of the functionals $\mathcal{F}, \mathcal{F}^{(-)}, \mathcal{F}^{(\pm)}$ is indefinite: for instance, $d^2\mathcal{F}(g) = 2\langle (x-s)h, h \rangle$. Nevertheless, the polynomials f_n^-, f_n^\pm have been proved [11] to be optimal in the following sense: for any $n \geq 1$ and all $f \in \Phi, \deg f \leq n$

$$\mathcal{F}(f_n) \geq \mathcal{F}(f).$$

3. Asymptotic bounds derived from (1) relying upon the polynomials f_n, f_n^-, f_n^\pm coincide. For the finite values of the parameters, better bounds are obtained from f_n^-, f_n^\pm .

3. Spectral method

This section is devoted to a different way of constructing polynomials for the Delsarte problem. The ideas discussed below originate in the work of C. Bachoc [12]. They were elaborated upon in an earlier work of the authors [2].

We develop the remark made after (6), namely that for any $i \geq 1$, $K_k(x, x_{k+1,i})$ is an eigenfunction of the Jacobi operator X_k . Since $K_k(x, s)$ is a good choice for the polynomial in Delsarte's problem, it is possible to construct polynomials as eigenvectors of X_k as opposed to the analytic arguments discussed above. In particular, $K_k(x, s)$ arises as an eigenfunction of the operator $T_k = T_k(s)$ defined by

$$\begin{aligned} T_k : V_k &\rightarrow V_k \\ \phi &\mapsto X_k \phi + \rho_k \hat{\phi}_k p_k \end{aligned}$$

where $\rho_k = a_k p_{k+1}(s)/p_k(s)$. Indeed, using (5) and (6) we obtain

$$(T_k - s)K_k(x, s) = (X_k - s)K_k(x, s) + a_k p_{k+1}(s)p_k(x) = 0.$$

On account of earlier arguments we should choose the polynomial for problem (1) in the form $F(x) = (x-s)f^2(x)$ where $f(x) = f(x, s)$ is an eigenfunction of T_k . The positive definiteness condition of f can be proved using the Perron-Frobenius theorem; for this we must take f to be the eigenfunction that corresponds to the *largest* eigenvalue of T_k . This condition defines the range of code distances s in which the method is applicable.

A variant of this calculation was performed in [2] to which we refer for details. The difference between [2] and the argument above is that there we

took $\rho_k = a_k p_{k+1}(1)/p_k(1)$. This has the advantage of defining T_k independently of s but leads to a bound of the form

$$|C| \leq \frac{4a_k p_{k+1}(1)p_k(1)}{1 - \lambda_k} \quad (10)$$

which is generally somewhat weaker than (8). Using the function F defined above we can improve this to recover the estimate (8).

We note that this argument does not depend on the choice of the functional space; in particular, the kernels K_k^-, K_k^\pm arise if the operator X_k is written with respect to the basis of the corresponding adjacent polynomials ($\{p_i^-\}$ or $\{p_i^\pm\}$) and their generating distribution. To conclude, Levenshtein's polynomials and bounds on codes can be derived within the framework of the spectral method.

Example 2.2. Consider again Example 2.1(a). The adjacent polynomials up to a constant factor that does not depend on i are given by [5, p.81]

$$p_i^-(x) = \tilde{k}_i^{(n-1)}(z), \quad p_i^\pm(x) = \tilde{k}_i^{(n-2)}(z) \quad \text{for } z = \frac{n}{2}(1-x) - 1,$$

where $\tilde{k}_i^{(n-1)}(z)$ for instance denotes the degree- i normalized Krawtchouk polynomial associated with the $(n-1)$ -dimensional Hamming space. The Jacobi matrix J_k for the basis p_i^- can be computed from (4) as follows. Since

$$xp_i^-(x) = \left(1 - \frac{2}{n}(z+1)\right)\tilde{k}_i^{(n-1)}(z),$$

we find that the coefficients of three-term recurrence for the family $\{p_i^-\}$ are

$$a_i = (1/n)\sqrt{(n-k-1)(k+1)}, \quad b_i = -1/n, \quad i = 0, 1, \dots$$

Constructing the operator T_k as described above, we obtain $K_k^-(x, s)$ as its eigenfunction. A similar construction can be pursued for the function K_k^\pm .

The approach outlined above has two advantages. First, it enables one to obtain simple estimates of the largest eigenvalue of X_k which is important in verifying the condition $f(x) \leq 0, x \in [-1, s]$. The second advantage is a more substantial one: this method can be extended to the case of *multivariate zonal polynomials* when the analytic alternative is not readily available. This case arises when the space \mathfrak{X} is homogeneous but not 2-point homogeneous. Worked examples include the real Grassmann manifold $G_{k,n}$ ([12]; the P_i are given by the generalized k -variate Jacobi polynomials) and

the so-called ordered Hamming space [3]. We provide a few more details on the latter case in order to illustrate the general method.

Let \mathcal{Q} be a finite alphabet of size q . Consider the set $\mathcal{Q}^{r,n}$ of vectors of dimension rn over \mathcal{Q} . A vector \mathbf{x} will be written as a concatenation of n blocks of length r each, $\mathbf{x} = \{x_{11}, \dots, x_{1r}; \dots; x_{n1}, \dots, x_{nr}\}$. For a given vector \mathbf{x} let $e_i, i = 1, \dots, r$ be the number of r -blocks of \mathbf{x} whose rightmost nonzero entry is in the i th position counting from the beginning of the block. The r -vector $e = (e_1, \dots, e_r)$ will be called the *shape* of \mathbf{x} . A shape vector $e = (e_1, \dots, e_r)$ defines a partition of a number $N \leq n$ into a sum of r parts. Let $e_0 = n - \sum_i e_i$. Let $\Delta_{r,n} = \{e \in (\mathbb{Z}_+ \cup \{0\})^r : \sum_i e_i \leq n\}$ be the set of all such partitions. The zonal polynomials associated to $\mathcal{Q}^{r,n}$ are r -variate polynomials $P_f(e), f, e \in \Delta_{r,n}$ of degree $\kappa = \sum_i f_i$. They are orthogonal on $\Delta_{r,n}$ according to the following inner product

$$\sum_{e \in \Delta_{r,n}} P_f(e) P_g(e) w(e) = 0 \quad (f \neq g).$$

The weight in this relation is given by the multinomial probability distribution

$$w(e_1, \dots, e_r) = n! \prod_{i=1}^r \frac{p_i^{e_i}}{e_i!} \quad (p_i = q^{i-r-1}(q-1), i = 1, \dots, r; p_0 = q^{-r}),$$

so the polynomials $P_f(e)$ form a particular case of *r-variate Krawtchouk polynomials*.

Let $\mathbf{x} \in \mathcal{Q}^{r,n}$ be a vector of shape e . Define a norm on $\mathcal{Q}^{r,n}$ by setting $w(\mathbf{x}) = \sum_i i e_i$ and let $d_r(\mathbf{x}, \mathbf{y}) = w(\mathbf{x} - \mathbf{y})$ be the ordered Hamming metric (known also as the Niederreiter-Rosenbloom-Tsfasman metric). We note that in the multivariate case there is no direct link between the variables and the metric. For instance, for the space $\mathcal{Q}^{r,n}$ the polynomials (as well as relations in the corresponding association scheme) are naturally indexed by shape vectors e while the weight is some function e .

The Delsarte theorem in this case takes the following form: *The size of an (n, M, d) code $C \subset \mathcal{Q}^{r,n}$ is bounded above by $M \leq \inf_{f \in \Phi} f(0)/f_0$, where*

$$\Phi = \left\{ f(x) = f(x_1, \dots, x_r) = f_0 + \sum_{e \neq 0} f_e P_e(x) : f_0 > 0, f_e \geq 0 (e \neq 0); \right. \\ \left. f(e) \leq 0 \quad \forall e \text{ s.t. } \sum_{i=1}^r i e_i \leq d \right\}$$

The argument for the univariate case given in this section can be repeated once we establish a three-term relation for the polynomials $P_f(e)$. Let \mathbb{P}_κ be

the column vector of the normalized polynomials P_f ordered lexicographically with respect to all f that satisfy $\sum_i f_i = \kappa$ and let $F(e)$ be a suitably chosen linear polynomial. Then

$$F(e)\mathbb{P}_\kappa(e) = A_\kappa\mathbb{P}_{\kappa+1}(e) + B_\kappa\mathbb{P}_\kappa(e) + A_{\kappa-1}^T\mathbb{P}_{\kappa-1}(e)$$

where A_κ, B_κ are matrices of order $\binom{\kappa+r-1}{r-1} \times \binom{\kappa+s+r-1}{r-1}$ and $s = 1, 0$, respectively. The elements of these matrices can be computed explicitly from combinatorial considerations. This gives an explicit form of the operator $S_\kappa = E_\kappa \circ F(e)$ in the orthonormal basis. Relying on this, it is possible to derive a bound on codes in the NRT space of the form (10) and perform explicit calculations, both in the case of finite parameters and for asymptotics. The full details of the calculations are given in [3].

Acknowledgments: The research of A. Barg is supported in part by NSF grants CCF0515124 and CCF0635271, and by NSA grant H98230-06-1-0044. The research of D. Nogin is supported in part by Russian Foundation for Basic Research through grants RFBR 06-01-72550-CNRS and RFBR 06-01-72004-MST. Parts of this research were presented at the International Workshop on Coding and Cryptology, The Wuyi Mountain, Fujian, China, June 11-15, 2007, and COE Conference on the Development of Dynamic Mathematics with High Functionality (DMHF2007), Fukuoka, Japan, October 1-4, 2007.

References

- [1] V. I. Levenshtein. Universal bounds for codes and designs. In V. Pless and W. C. Huffman, Eds., *Handbook of Coding Theory*, vol. 1, pp. 499–648. Elsevier Science, Amsterdam, (1998).
- [2] A. Barg and D. Nogin, Spectral approach to linear programming bounds on codes, *Problems of Information Transmission*. **42**, 12–25, (2006).
- [3] A. Barg and P. Purkayastha, Bounds on ordered codes and orthogonal arrays. arxiv:CS/0702033.
- [4] V. I. Levenshtein. On choosing polynomials to obtain bounds in packing problems. In *Proc. 7th All-Union Conf. Coding Theory and Information Transmission, Part 2*, pp. 103–108, Moscow, Vilnius, (1978). (In Russian).
- [5] V. I. Levenshtein, Bounds for packings of metric spaces and some of their applications, *Problemy Kibernet.* **40**, 43–110 (In Russian), (1983).
- [6] V. I. Levenshtein, Designs as maximum codes in polynomial metric spaces, *Acta Appl. Math.* **29**(1-2), 1–82, (1992). ISSN 0167-8019.
- [7] G. Andrews, R. Askey, and R. Roy, *Special functions*. (Cambridge University Press, 1999).
- [8] M. G. Kreĭn and A. A. Nudel'man, *The Markov moment problem and extremal problems*. (American Mathematical Society, Providence, R.I., 1977).

- [9] R. J. McEliece, E. R. Rodemich, H. Rumsey, and L. R. Welch, New upper bound on the rate of a code via the Delsarte-MacWilliams inequalities, *IEEE Trans. Inform. Theory*. **23**(2), 157–166, (1977).
- [10] G. A. Kabatiansky and V. I. Levenshtein, Bounds for packings on the sphere and in the space, *Problems of Information Transmission*. **14**(1), 3–25, (1978).
- [11] V. M. Sidelnikov, Extremal polynomials used in bounds of code volume, *Problemy Peredachi Informatsii*. **16**(3), 17–30, (1980).
- [12] C. Bachoc, Linear programming bounds for codes in Grassmannian spaces, *IEEE Trans. Inform. Theory*. **52**, 2111–2126, (2006).